



UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE  
United States Patent and Trademark Office  
Address: COMMISSIONER OF PATENTS AND TRADEMARKS  
Washington, D.C. 20231  
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
08/994,878	12/19/1997	MICHAEL A. EPSTEIN	PHA-23.313	7153

7590                    09/26/2002

JACK E HAKEN  
US PHILIPS CORP  
INTELLECTUAL PROP DEPT  
580 WHITE PLAINS ROAD  
TARRYTOWN, NY 10591

[REDACTED] EXAMINER

SONG, HOSUK

[REDACTED] ART UNIT      [REDACTED] PAPER NUMBER

2131

DATE MAILED: 09/26/2002

21

Please find below and/or attached an Office communication concerning this application or proceeding.

7/21

## Office Action Summary

Application No. <b>08/994,878</b>	Applicant(s) <b>EPSTEIN</b>
Examiner <b>HO S. SONG</b>	Art Unit <b>2131</b>

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

### Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136 (a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133).
- Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

### Status

1)  Responsive to communication(s) filed on Jul 29, 2002

2a)  This action is FINAL.      2b)  This action is non-final.

3)  Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11; 453 O.G. 213.

4)  Claim(s) 1-20 is/are pending in the application.

4a) Of the above, claim(s) 1-4 and 9-20 is/are withdrawn from consideration.

5)  Claim(s) \_\_\_\_\_ is/are allowed.

6)  Claim(s) 5-8 is/are rejected.

7)  Claim(s) \_\_\_\_\_ is/are objected to.

8)  Claims \_\_\_\_\_ are subject to restriction and/or election requirement.

### Application Papers

9)  The specification is objected to by the Examiner.

10)  The drawing(s) filed on \_\_\_\_\_ is/are a)  accepted or b)  objected to by the Examiner.  
Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

11)  The proposed drawing correction filed on \_\_\_\_\_ is: a)  approved b)  disapproved by the Examiner.  
If approved, corrected drawings are required in reply to this Office action.

12)  The oath or declaration is objected to by the Examiner.

### Priority under 35 U.S.C. §§ 119 and 120

13)  Acknowledgement is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).  
a)  All b)  Some\* c)  None of:  
1.  Certified copies of the priority documents have been received.  
2.  Certified copies of the priority documents have been received in Application No. \_\_\_\_\_.  
3.  Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

\*See the attached detailed Office action for a list of the certified copies not received.

14)  Acknowledgement is made of a claim for domestic priority under 35 U.S.C. § 119(e).  
a)  The translation of the foreign language provisional application has been received.

15)  Acknowledgement is made of a claim for domestic priority under 35 U.S.C. §§ 120 and/or 121.

### Attachment(s)

1)  Notice of References Cited (PTO-892)      4)  Interview Summary (PTO-413) Paper No(s). \_\_\_\_\_

2)  Notice of Draftsperson's Patent Drawing Review (PTO-948)      5)  Notice of Informal Patent Application (PTO-152)

3)  Information Disclosure Statement(s) (PTO-1449) Paper No(s). \_\_\_\_\_      6)  Other: \_\_\_\_\_

Art Unit: 2131

## **DETAILED ACTION**

### ***Claim Rejections - 35 USC § 103***

- 1 The text of those sections of Title 35, U.S. Code not included in this action can be found in a prior Office action.
- 2 Claims 5,7 remain rejected under 35 U.S.C. 103(a) as being unpatentable by Trostle(US 5,919,257) in view of Asay et al.(US 5,903,882).

In claim 5, Trostle teaches user transmitting ID over the network in (col.5, lines 50-51). Trostle discloses reading from a storage data corresponding to the user having the received ID, which data comprises the user's private key encrypted using a key determined from identifying information of the user and sending via network the encrypted private key, whereby the encrypted key can be received and decrypted at the location of the user's identifying information in (col.5, lines 51-57). Trostle does not discloses destroying any non-volatile record of the private key at the location of the user. Asay disclose in (col.30, lines 55-57 and col.55, lines 38-43) where after application is signed by a private key, private key is destroyed at the user's site. It would have been obvious to person of ordinary skill in the art at the time invention was made to destroy a private key at the user's site taught in Asay with a public key system disclosed in Trostle in order to assure the user that private key is no longer available for access if attempted by the hackers and

Art Unit: 2131

since private key is discarded at user's site, the user has total control of its key rather than key handled at the remote site where it can be viable for attacks.

In claim 7, the examiner takes official notice that hashing a document is well known in the art. The most common cryptographic uses of hash functions are with digital signatures and for data security. One of ordinary skill in the art would be motivated to use hash function in order to save both time and space.

3. Claims 6,8, remain rejected under 35 U.S.C. 103(a) as being unpatentable over Trostle in view of Schneier and further in view of Asay.

In claims 6,8, Trostle discloses all the limitations above. However, Trostle does not disclose Passphrase scheme. Schneier discloses passphrase scheme in (page 174, passphrase section). It would have been obvious to one of ordinary skill in the art at the time the invention was made to use passphrase taught in Schneier for password of Trostle so that user can remember phrases easier than random character sequences. Passphrase provides greater security through increased entropy than a short password. Trostle/Schneier does not disclose processing user's approval of the document. Asay's patent disclose digitally signing a user's approval document using a private key. It would have been obvious to person of ordinary skill in the art at the time invention was made to have approval/validation process done by the user as taught in Asay with validation process disclosed in Trostle so that if the system is idle or left unattended by the user any intruders or hackers can compromise the system. Manual validation process such as digital signing of the document done by the user assures security. The examiner takes official notice that

Art Unit: 2131

hashing a document is well known in the art. The most common cryptographic uses of hash functions are with digital signatures and for data security. One of ordinary skill in the art would be motivated to use hash function in order to save both time and space.

***Response to Applicant's Arguments***

4. Claims 1-2,11-16,19 has been canceled.
5. ***Applicant has argued that*** Asay teaches the destruction of a private, and subsequent reconstruction of the key in order to from the user's private key but in Asay (col 30, lines 53-54) "the corresponding private key is stored in a safe place in the subscriber's system" and follow with "the subscriber mechanism 106 then unwraps the private key stored away for use in the event that a certificate is issued based on the standby application". ***In response:*** the Applicant is claiming in claim 5, "***destroying or*** avoiding making any non-volatile record of the private key at the location of the user". Even though Asay patent teaches storing the corresponding private key in the subscriber's system. Destroying the private key in subscriber's system is specifically disclosed by Asay. Applicant ***is claiming destroying private key*** at the user's site only and does not claim complete deletion/erase/destroy of all key copy in user's system.. Therefore it meets the claim limitation. ***Applicant argues that*** the entire premise of the Applicant's invention is to assure the presence of the user, by requiring the user to initiate some identifying action for each security transaction and Trostle's system is a "transparent to the user". ***In response:*** the Applicant is arguing which are not claimed or reflected in the claim language. Applicant has argued that

Art Unit: 2131

private key is not the user's private key. In response: the examiner disagree, the private key disclosed by Asay is user's private key(see col.7,lines 46-50).

***Conclusion***

6       **THIS ACTION IS MADE FINAL.** Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within TWO MONTHS of the mailing date of this final action and the advisory action is not mailed until after the end of the THREE-MONTH shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the mailing date of this final action.

7.       Any inquiry concerning this communication should be directed to Ho S. Song at telephone number (703)305-0042. The examiner can normally be reached on Monday through Friday from 6:00 am to 4:30 pm.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Gail Hayes, can be reached at (703)305-9711.

Art Unit: 2131

Any inquiry of a general nature or relating to the status of this application or preceding  
should be directed to the group receptionist, whose telephone number is (703)305-3900.

*Ho Song*

*Gail Hayes*  
GAIL HAYES  
SUPERVISORY PATENT EXAMINER  
TECHNOLOGY CENTER 2100